IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

JUAN ORTEGA, DAVID MERKLE, and NANCY MERKLE, on behalf of themselves and all others similarly situated, Plaintiffs, v. **PROGRESS SOFTWARE CORPORATION**, a Delaware Publicly Traded Corporation; **PENSION BENEFIT INFORMATION, LLC**, a Delaware Limited Liability Company, Defendants.	Case No. **COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs JUAN ORTEGA, DAVID MERKLE, and NANCY MERKLE ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against PROGRESS SOFTWARE CORPORATION (hereinafter "PROGRESS") and PENSION BENEFIT INFORMATION, LLC (hereinafter "PBI") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. BACKGROUND / INTRODUCTION

1. Plaintiffs bring this class action against PROGRESS and PBI for their failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' names, addresses, Social Security numbers, birthdates, demographic information, beneficiaries'

information, driver's license numbers, vehicle registration numbers, and other personally identifiable information and financial information (collectively, the "Private Information").

2. Plaintiffs are, and at all material times were, retirees and recipients of pension benefits through the California Public Employment Retirement System and the California State Teachers Retirement System (collectively, the "Retirement Systems")

3. The Retirement Systems contracted with Defendant PBI to provide certain services in furtherance of administration of the Retirement Systems.

4. Defendant PROGRESS is a software company offering a range of products and services to government and corporate entities across the country and around the world.

5. "Private Information" was shared between the Retirement Systems and PBI using PROGRESS's proprietary line of products and services, including file transfer software, file transfer services, cloud hosting, and /or cloud storage known as "MOVEit," "MOVEit File Transfer," and "MOVEit Cloud" (hereinafter the "MOVEit Software").

6. On or about May 31, 2023, PROGRESS posted on its website a "Critical Vulnerability" notice, stating, in part: "PROGRESS has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment." A nearly identical notice was posted with regard to MOVEit Cloud.

7. On or about June 6, 2023, a Russian based cyber terrorist group named "CLOP" has publicly claimed to have accessed and retrieved the Private Information of millions of americans, using the critical vulnerabilities in the MOVIEit Software.

8. Since June 6, 2023, additional critical vulnerabilities in MOVEit Software have been identified and publicly admitted to by PROGRESS.

9. PROGRESS and PBI have not yet sent direct notice to those impacted by the Data Breach, though many of Defendants' customers, including the Retirement Systems, have begun notifying individuals, that their Private Information has been compromised as a result of the Breach.

10. PROGRESS has not confirmed that it has adequately enhanced its data security practices sufficient to avoid a similar vulnerability in its "MOVEit Software" in the future.

11. PROGRESS has not confirmed to Plaintiffs and Class members what if any negotiations took place with CLOP, and what, if any of the Private Information was sold, released, publicized, etc.

12. Plaintiffs and Class Members have suffered and continue to suffer harm, including release of the Private Information, imminent risk of identity theft and other fraudulent misuse of the Private Information by bad actors, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. Plaintiffs bring this class action lawsuit to address the inadequate safeguarding of Plaintiffs and Class Members' Private Information maintained and shared by and between Defendants through the MOVEit Software and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the Private Information accessed, and that such information was subject to unauthorized access by cybercriminals.

14. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants shared, collected and maintained is

now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

16. Plaintiff Juan Ortega is, and at all times mentioned herein was, an individual citizen of the State of California and resides within the District.

17. Plaintiff Juan Ortega is, and at all times mentioned herein was, a retiree receiving benefits through the California Public Employees' Retirement System (hereinafter "CalPERS")

18. Plaintiff David Merkle is, and at all times mentioned herein was, an individual citizen of the State of California.

19. Plaintiff David Merkle is, and at all times mentioned herein was, a retiree receiving benefits through the California State Teachers' Retirement System (hereinafter "CalSTRS")

20. Plaintiff Nancy Merkle is, and at all times mentioned herein was, an individual citizen of the State of California.

21. Plaintiff Nancy Merkle is, and at all times mentioned herein was, a retiree receiving benefits through the California State Teachers' Retirement System (hereinafter "CalSTRS").

22. Defendant PROGRESS (hereinafter "PROGRESS") is and at all times mentioned herein was, a publicly traded software company formed in the state of Delaware, headquartered

at 15 Wayside Road, Suite 4, Burlington, Massachusetts, and doing business within the State of California as "CSC – Lawyers Incorporating Service" pursuant to California Corporations Code Section 1505.

23. Defendant Pension Benefit Information, LLC (hereinafter "PBI") is and at all times mentioned herein was, a private research company formed in the state of Delaware, headquartered at 333 S 7th Street Ste 2400 Minneapolis, Minnesota, and doing business within the State of California as "CSC – Lawyers Incorporating Service" pursuant to California Corporations Code Section 1505.

III. JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has jurisdiction over PROGRESS because PROGRESS operates in and/or is incorporated in this District, and conducts regular business within this District.

26. This Court has jurisdiction over PBI because PBI operates in and/or is incorporated in this District, and conducts regular business within this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and PROGRESS has harmed Class Members residing in this District, including Plaintiff Juan Ortega.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial

part of the events giving rise to this action occurred in this District and PBI has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and PBI has harmed Class Members residing in this District, including Plaintiff Juan Ortega.

30. The Retirement Systems administering and operating the pension funds for millions of Californians, including Plaintiffs' and Class Members', contracted with Defendant PBI, LLC to conduct research into retirees and beneficiaries for the purpose of locating and confirming vital statistics and information relating to said persons, including but not limited to current addresses, proper beneficiary information, and mortality.

31. Defendant PROGRESS is a private software company offering a range of products and services to government and corporate entities across the country and around the world.

32. Defendant PBI contracted with, purchased from, and/or otherwise utilized and relied upon Defendant PROGRESS' product for the purpose of sharing files to/from the Retirement Systems, including the "Private Information" of more than two (2) million retirees.

33. As a condition of receiving secure file transfer services, Defendants require that its government and corporate customers entrust them with highly sensitive personal information belonging to individuals like Plaintiffs.

34. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants promise to, among other things: keep customers' files private; comply with industry standards related to data security and the maintenance of its customers' files and the Private Information contained therein; only use and release highly

sensitive information stored on its servers for reasons that relate to the services it provides; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

36. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

A. <u>The Breach</u>

37. On or about May 31, 2023, PROGRESS posted on its website a "Critical Vulnerability" notice, stating, in part: "PROGRESS has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment." A nearly identical notice was posted with regard to MOVEit Cloud.

38. As a result of the vulnerabilities within PROGRESS's proprietary products and services, including vulnerabilities in its coding that were identifiable to cybersecurity experts conducting an investigation after the fact, the "Private Information" of millions of persons was accessed and collected by unauthorized third-part(ies) ("The Breach").

39. On information and belief, "CLOP" is a Russian based group that has previously admitted to being the perpetrator of several large data hacks and malware/ransomware attacks in

the United States in recent history. CLOP's modus operandi is that the group steals highly sensitive information by exploiting vulnerabilities in software, products, systems, etc and then demands a ransom to be paid for said information to be returned and for assurances that it will not be distributed publicly.

40. On or about June 6, 2023, "CLOP" claimed credit for the Breach that is the basis for the instant action and posted a ransom note indicating the Private Information would be publicly released and/or otherwise sold, exploited, used maliciously, if its demands were not met within ten (10) days' time.

41. CLOP stated that it would reveal to those companies it negotiates with information amounting to ten percent (10%) of what it stole from Defendants and, in turn, Plaintiffs' and Class Members, as an offer of proof that it did in fact steal the "Private Information."

42. On or about June 9, 2023, Defendant PROGRESS posted an additional notice on its website that states, in pertinent part: "In addition to the ongoing investigation into vulnerability (CVE-2023-34362), we have partnered with third-party cybersecurity experts to conduct further detailed code reviews as an added layer of protection for our customers. As part of these code reviews, cybersecurity firm Huntress has helped us to uncover additional vulnerabilities that could potentially be used by a bad actor to stage an exploit. These newly discovered vulnerabilities are distinct from the previously reported vulnerability shared on May 31, 2023."

43. On or about June 15, 2023, Defendant PROGRESS posted an additional notice on its website indicating that vulnerabilities had been addressed and that the MOVEit Software "has been patched and fully restored" including a patch to "address a newly identified vulnerability."

44. On or about June 18, 2023, Defendant PROGRESS posted an additional notice on its website that states, in pertinent part:

> i. We have not seen any evidence that the vulnerability reported on June 15 has been exploited. Taking MOVEit Cloud offline for maintenance was a defensive measure to protect our customers and not done in response to any malicious activity. Because the new vulnerability we reported on June 15 had been publicly posted online, it was important that we take immediate action out of an abundance of caution to quickly patch the vulnerability and disable MOVEit Cloud.
>
> ii. Our product teams and third-party forensics partner have reviewed the vulnerability and associated patch and have deemed that the issue has been addressed. This fix has been applied to all MOVEit Cloud clusters and is available for MOVEit Transfer customers.
>
> iii. A third party publicly disclosed a vulnerability impacting MOVEit Transfer and MOVEit Cloud in a way that did not follow normal industry standards, and in doing put our customers at increased risk of exploitation. Because it is common across the industry that reported vulnerabilities lead to increased attention from both malicious threat actors and cybersecurity researchers trying to uncover new vulnerabilities, we are working closely with our industry partners to take all appropriate steps to address any issues.

45. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

46. Plaintiffs and Class Members permitted their Private Information to be provided to the Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

47. PROGRESS' data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same bad actor: "CLOP".

48. Thus, PROGRESS knew or should have known that its electronic records would be targeted by cybercriminals and taken precautions, particularly following recent breaches in the industry.

49. Upon Information and belief, PROGRESS had notice of vulnerabilities in its MOVEit Software and, specifically, SQL injection vulnerability, dating back as far as 2021.

50. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to PROGRESS, and thus PROGRESS was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

51. Upon information and belief, PROGRESS failed to both properly monitor and properly implement data security practices with regard to the computer network and systems that housed the Private Information. Had PROGRESS properly monitored its networks, it would have discovered the vulnerabilities and the eventual Data Breach sooner.

52. Only <u>following</u> the Breach did PROGRESS hire experts to review its coding and additional "critical" vulnerabilities were discovered.

53. Defendants have not yet sent direct notice to those impacted by the Data Breach, though many of Defendants' customers, including the Retirement Systems, have begun notifying individuals, that their Private Information has been compromised as a result of the Breach.

54. PROGRESS has not confirmed that it has adequately enhanced its data security practices sufficiently to avoid a similar vulnerability in its "MOVEit Software" in the future.

55. PBI has not confirmed that it has removed the Private Information from the MOVEit Software or otherwise taken steps to ensure that PROGRESS vulnerabilities do not cause further harm to Plaintiffs and Class members.

56. Defendants have not confirmed to Plaintiffs and Class members what if any negotiations took place with CLOP, and what, if any of the Private Information was sold, released, publicized, etc.

57. Now, thirty days following the Data Breach, neither Defendant has directly notified those persons who's Private information was stolen in the Data Breach, leaving it to the public agencies that entrusted Defendants with Private Information to notify those affected instead, causing significant delay in notice to persons affected that their information was stolen by a Russian malware ransom group. Said direct notice is critical to ensuring affected persons can take proper steps to monitor and secure their accounts and identity.

B. Failure To Comply With Federal Guidelines

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

59. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45(a)(1) provides that "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."

60. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, *understand their network's vulnerabilities*, and implement policies to correct any security problems. The guidelines also recommend that businesses

use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

61. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. As evidenced by the Breach and the identification of critical vulnerabilities in its coding by at least two third parties other than PROGRESS itself, PROGRESS failed to properly implement basic data security practices.

64. PROGRESS' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

65. PROGRESS was at all times fully aware of its obligation to protect the Private Information of Plaintiffs and Class Members yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

C. Failure To Comply With Industry Standards

66. Technology and Cyber Security Industry Standards include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data, installing appropriate malware detection software, monitoring and limiting network ports, protecting web browsers and email management systems, setting up network systems such as firewalls, switches, and routers, monitoring and protecting physical security systems, and protocol for regularly investigating potential vulnerabilities.

67. PROGRESS failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

68. PROGRESS was on notice of a possible critical vulnerability as far back as 2021.

69. PROGRESS was on notice that CLOP was engaging in major ransomware attacks and theft of confidential personal information in early 2023.

70. PROGRESS failed to comply with these accepted standards, thereby permitting the Breach to occur.

71. Following the Breach, PROGRESS regularly identified additional vulnerabilities for weeks thereafter, all of which could and should have been discovered and fixed prior to exploitation and theft by CLOP.

D. Defendants' Breach Of Duty To Safeguard Information

72. In addition to PROGRESS' obligations under federal and state laws, Defendants both owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, sharing, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

73. PBI owed a duty to Plaintiffs and Class Members to ensure any company it provided their Private Information to would exercise due care in the handling and safeguarding of said information, provide reasonable security, including complying with industry standards and all legal requirements, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

74. PROGRESS owed a duty to Plaintiffs and Class Members to ensure the Private Information with which it was entrusted by PBI was protected and, further, owed a duty to Plaintiffs and Class Members to exercise due care in the handling and safeguarding of said information, provide reasonable security, including complying with industry standards and all legal requirements, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

75. Defendants, and each of them, breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard Private Information.

76. PROGRESS' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk

of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing vulnerabilities and/or intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers' files containing the Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

77. PBI negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by not ensuring that the company to which it entrusted Plaintiffs' and Class Members' Private Information, <u>and to whom it transferred said information intentionally</u>, was operating within industry standards, in compliance with all federal and state laws, to secure Plaintiffs' and Class Members' Private Information.

78. PROGRESS negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network, systems, and servers which contained unsecured and unencrypted Private Information, due to its failure to operate and secure said Private Information within Industry Standards, Federal and State law.

79. Had PROGRESS remedied the deficiencies and vulnerabilities in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented intrusion into its information

storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

80. Further, PROGRESS and PBI breached a duty owed to Plaintiffs and Class Members when they each failed to send notice to Plaintiffs and Class Members directly to alert them about the Breach and the theft of their Private Information.

E. <u>PROGRESS Should Have Known That Cybercriminals Target Private Information</u>

81. The FTC has acknowledged and, in fact, lectured in its workshops to Industry professionals about "informational injuries."

82. Informational Injuries are those that occur when private individuals and consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data. FTC acknowledges expressly and teaches Industry professionals that such injuries can cause loss of employment, loss of ability to obtain employment, loss of trust in e-commerce, and deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life. All of these informational injuries apply to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are affected by a loss of trust in the governmental agency in charge of Plaintiffs and Class Members' retirement funds.

83. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

84. A person's identity is akin to a puzzle. Thus, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

85. As technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

86. Thus, even if certain information was not purportedly involved in the Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

87. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity),

reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[5] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

88. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to- reward analysis illustrates beyond doubt that PII has considerable market value.

89. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

90. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy.

91. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

92. The theft of Plaintiffs' and Class Members' Private Information is a loss of valuable property with long reaching effects, particularly if immediate steps to secure accounts and monitor credit are not taken.

93. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

94. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

F. Plaintiffs' And Class Members' Damages

95. Plaintiffs are residents of the State of California and each are retirees of the Retirement Systems that transferred information to PBI using PROGRESS' vulnerable and ultimately exploitable MOVEit Software.

96. On or about June 29, 2023, Plaintiffs received notice of the Data Breach from the Retirement Systems and/or publicly available information regarding the Data Breach alerting them of the Data Breach and that their Private Information was at risk.

97. PROGRESS and PBI have neither sent direct notice of the Breach to those impacted nor has it provided any remedial services, such as free credit monitoring, to those affected by the Data Breach.

98. The Retirement Systems have begun to alert affected retirees and are offering free credit monitoring in certain circumstances, but are only just beginning this process weeks after the Breach and, due to Defendants' inaction, on information and belief, public funds are being used by the Retirement Systems to provide said monitoring for a one year time period.

99. But for PROGRESS' and PBI's delayed action and failure to act in swiftly notifying the impacted persons directly, remedial steps and precautions could already have been taken. The number of ways in which each Plaintiffs' and Class Members' Private Information could have been used at this point is nearly infinite.

100. Defendants have made no offers of credit monitoring or identity theft insurance

to Plaintiffs, Class Members or anyone else affected by the Breach.

101. Plaintiffs have suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach.

102. Plaintiffs would not have permitted that their Private Information be provided by the Retirement Systems to Defendants had Defendants timely disclosed that PROGRESS' file transfer servers lacked adequate data security to safeguard its customers' files and the highly sensitive personal information therein from theft, and that those servers were subject to a data breach.

103. Plaintiffs suffered actual injury in the form of having their Private Information compromised and/or stolen as a result of the Data Breach.

104. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Private Information – a form of intangible property that Plaintiffs entrusted to Defendants.

105. Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being placed in the hands of criminals.

106. Plaintiffs each have a continuing interest in ensuring that their Private Information, which remains on PROGRESS' MOVEit servers and stored within Defendants' systems, is protected and safeguarded from future breaches.

107. As a result of the Breach, Plaintiffs have already made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching long-term credit monitoring options they will now need to

use. Plaintiffs have spent several hours dealing with the Data Breach, valuable time they otherwise would have spent on other activities.

108. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their Private Information to cybercriminals, which Private Information they believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of committing cyber and other crimes against them. Plaintiffs are very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on their lives.

109. Plaintiffs also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from them; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud they now face.

110. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

111. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

112. Plaintiffs and Class Members entrusted their Private Information to the Retirement Systems as a condition of receiving their pension benefits. In turn, the Retirement Systems were authorized by Plaintiffs and Class Members to transfer the data

as needed to administer the pension fund to outside vendors, including PBI (and thereby also PROGRESS) in reliance upon assurances made by PBI and PROGRESS that the information would be held safe in accordance with industry standards and legal requirements.

113. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from PROGRESS' inadequate data security practices.

114. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of fraud and identity theft.

115. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

116. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

117. Additionally, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes"

and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

118. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was accessed, viewed, and acquired by CLOP.

119. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

120. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

121. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited

accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

122. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password- protected, and that such data is properly encrypted.

123. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

124. Plaintiffs bring this action individually and on behalf of all other persons

similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

125. Specifically, Plaintiffs propose the following Nationwide Class (referred to herein as the "Class" or "Class Members"), subject to amendment as appropriate:

a. Nationwide Class

i. All individuals in the United States whose Private Information was stored/accessible by Pension Benefit Information, LLC and compromised as a result of exploitation of Progress Software Corporation's MOVEit Transfer and MOVEit Cloud vulnerabilities.

126. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

127. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

128. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

129. Numerosity. The Class Members are so numerous that joinder of all members is

130. impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class likely consists of millions of individuals whose data was compromised in the Data Breach. The identities of Class

Members are ascertainable through PBI's and PROGRESS' records, Class Members' records, publication notice, self-identification, and other means.

131. Commonality. There are questions of law and fact common to the Class which

132. predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether PROGRESS engaged in the conduct alleged herein;
b. When PROGRESS learned of the Data Breach;
c. Whether PBI engaged in the conduct alleged herein;
d. When PBI learned of the Data Breach;
e. Whether PBI's response to the Data Breach was adequate;
f. Whether PROGRESS' response to the Data Breach was adequate;
g. Whether PROGRESS unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
h. Whether PROGRESS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
i. Whether PROGRESS' data security practices related to its secure file transfer services prior to and during the Data Breach complied with applicable data security laws and regulations;
j. Whether PROGRESS' data security practices related to its secure file transfer services prior to and during the Data Breach were consistent with industry standards;
k. Whether PROGRESS owed a duty to Class Members to safeguard their Private Information;
l. Whether PROGRESS breached its duty to Class Members to safeguard their Private Information;
m. Whether PBI owed a duty to Class Members to safeguard their Private Information;
n. Whether PBI breached its duty to Class Members to safeguard their Private Information;
o. Whether hackers obtained Class Members' Private Information via the Data Breach;
p. Whether PROGRESS had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
q. Whether PROGRESS breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
r. Whether PBI had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
s. Whether PBI breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

t. Whether PROGRESS knew or should have known that its data security systems and monitoring processes as such relate to its secure file transfer services were deficient;

u. Whether PBI knew or should have known that PROGRESS' data security systems and monitoring processes as such relate to its secure file transfer services were deficient;

v. What damages Plaintiffs and Class Members suffered as a result of PROGRESS' misconduct;

w. Whether PROGRESS' conduct was negligent;

x. Whether PBI's conduct was negligent;

y. Whether PROGRESS' conduct was *per se* negligent;

z. Whether PROGRESS was unjustly enriched;

aa. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

bb. Whether Plaintiffs and Class Members are entitled to credit or identity monitoring and monetary relief; and

cc. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

133. Typicality. Plaintiffs' claims are typical of those of other Class Members because

134. Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

135. Adequacy of Representation. Plaintiffs will fairly and adequately represent and

136. protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

137. Predominance. PROGRESS and PBI have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from PROGRESS' and PBI's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

138. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PROGRESS. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

139. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). PROGRESS and PBI have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

140. Finally, all members of the proposed Class are readily ascertainable. PROGRESS has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PBI and PROGRESS.

VI. CLAIMS FOR RELIEF

A. COUNT I

NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class as against all Defendants)

141. Plaintiffs restate and reallege all of the allegations stated above as if fully set

forth herein.

142. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

143. PROGRESS' duty also included a responsibility to implement processes by which it could detect and analyze vulnerability of its systems quickly and to give prompt notice to those affected in the case of a cyberattack.

144. PROGRESS knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. PROGRESS was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

145. PBI's duty included a responsibility to inquire of PROGRESS with respect to its implementation of processes by which PROGRESS could detect and analyze vulnerability of its systems quickly and to give prompt notice to those affected in the case of a cyberattack, prior to utilizing PROGRESS' MOVEit Software in a manner that subjected Plaintiffs' and Class Members' Private Information to potential exposure.

146. PBI knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. PBI was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

147. PBI accepted Plaintiffs' and Class Members' Private Information by and through the Retirement Systems and thereby warranted that it would ensure the information was

kept confidential and in a manner that would shield it from a breach like the one that ultimately did occur.

148. PBI's duty of reasonable care in oversight of PROGRESS' security protocols was ongoing throughout the entirety of time that it had stored and/or maintained access to the Private Information of Plaintiffs and Class Members and continues to this day, given that PBI has not provided any notice that Plaintiffs' and Class Members' information is no longer stored and/or maintained in a manner that subjects it to access via PROGRESS' MOVEit Software vulnerabilities.

149. PROGRESS owed a duty of care, and continues to owe a duty of care, to Plaintiffs and Class Members whose Private Information was entrusted to it. PROGRESS's duties included/include, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;
e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

150. PROGRESS's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

151. PROGRESS's duty also arose because PROGRESS was bound by industry

standards to protect its customers' confidential Private Information.

152. PBI and PROGRESS' duties also arose by implied warranty and contractual obligations in place for the benefit of Plaintiffs and Class Members

153. PBI and PROGRESS' duties also arose out of common law duties of reasonable care with respect to property with which they were entrusted.

154. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

155. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession.

156. PROGRESS, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

157. Defendants, by their actions and/or omissions, breached their duties of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

158. PROGRESS breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

159. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

a. Failing to adequately monitor the security of its networks and systems;
b. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
c. Allowing unauthorized access to Class Members' Private Information;
d. Failing to comply with the FTCA;
e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

160. Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

161. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to turn over their Private Information to Defendants by and through the Retirement Systems was predicated on the understanding that Defendants would take adequate security precautions to protect it. Moreover, only Defendants had the ability to protect its systems (and the Private Information stored thereon) from attack.

162. Defendants' breach of duties owed to Plaintiffs and Class Members caused

Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

163. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

164. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

165. As a result of Defendants' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

166. Defendants' also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

167. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

168. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

169. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

170. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants' to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

B. <u>COUNT II</u>
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Nationwide Class as against all Defendants)

171. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

172. Upon information and belief, PBI entered into contracts with its government and corporate entity customers to provide research services to the Retirement Systems for the purpose of assisting in the administration and operation of the Retirement Systems. PBI knew that as part of its contractual obligations with the Retirement Systems and/or the State of California, it would require PBI to be entrusted with highly sensitive Private Information that it had a contractual obligation to safeguard.

173. Upon information and belief, PROGRESS entered into contracts with its government and corporate entity customers to provide secure file transfer services to them, which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

174. The contracts between the Retirement Systems and PBI were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were

direct and express beneficiaries of such contracts.

175. The contracts between PBI and PROGRESS were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

176. PROGRESS and PBI knew that if it were to breach these contracts with its customers, Plaintiffs and the Class, would be harmed.

177. PROGRESS and PBI breached its contracts with its customers and, as a result, Plaintiffs and Class Members were affected by this Data Breach when PROGRESS failed to use reasonable data security measures that could have prevented the Data Breach and when PBI failed to ensure that it was entrusting the Private Information to someone that would comply with all industry standards, federal and state regulations.

178. As foreseen, Plaintiffs and the Class were harmed by Defendants' failures, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

179. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

C. <u>COUNT III</u>

UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

180. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

181. Plaintiffs and Class Members conferred a benefit on PROGRESS by turning over their Private Information to Defendant through the Retirement Systems and/or PBI.

182. Plaintiffs and Class Members conferred a benefit on PBI by turning over their Private Information to Defendant through the Retirement Systems.

183. Upon information and belief, PROGRESS funds its business and enjoys a profit from said business entirely from its general revenue, including from payments made to it by its government and corporate entity customers.

184. Upon information and belief, PROGRESS funds the creation, implementation, and costs of its data security measures and protocols entirely from its general revenue, including from payments made to it by its government and corporate entity customers.

185. As such, a portion of the payments made to PROGRESS and PBI by their customers, which payments would not be possible without Plaintiffs and Class Members turning over their Private Information, is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to PROGRESS.

186. Upon information and belief, PBI operates a private business of data analysis and research relating directly to the Private Information of Plaintiffs and Class Members. To conduct its business, accessing and maintaining the Private Information of Plaintiffs and Class Members was a vital, integral, and necessary part of PBI's business, which Private Information PBI was obligated to maintain securely and safely. The cost of storing and maintaining the Private Information was funded entirely from its general revenue, including from payments made to it by its government and corporate entity

customers.

187. As such, a portion of the payments made to both Defendants by their customers, which payments would not be possible without Plaintiffs and Class Members turning over their Private Information, is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

188. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from its customers that should have been used for adequate cybersecurity practices that it failed to provide.

189. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

190. If Plaintiffs and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information.

191. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of its wrongful conduct.

192. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class

Members have suffered and/or are at a substantial and continuing risk of suffering injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

193. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

194. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

D. <u>COUNT IV</u>

DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class against all Defendants)

195. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

196. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the FTCA, common law, and industry standards described in this Complaint.

197. Defendants owed a duty of care to Plaintiffs and Class Members, which required each of them to adequately secure Plaintiffs' and Class Members' Private Information.

198. Defendants still possess Private Information regarding Plaintiffs and Class Members.

199. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

200. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure its customers' files storing the Private Information belonging to Plaintiffs and Class Members, and to timely notify Plaintiffs and Class Members of the Data Breach and future data breaches under the common law and Section 5 of the FTCA;

b. Defendants' existing security measures did not, and do not, comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' files that store Plaintiffs' and Class Members' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

201. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. PROGRESS engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PROGRESS's systems on a periodic basis, and ordering PROGRESS to promptly correct any problems or issues detected by such third-party security auditors;

ii. PROGRESS engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. PROGRESS auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. PROGRESS segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of PROGRESS's systems;

v. PROGRESS regular database scanning and security checks;

vi. PROGRESS routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. PBI routinely and continually conducting inspections and audits on PROGRESS' internal security protocols and processes to ensure that the above security measures have actually been implemented and continuously executed by PROGRESS; and

viii. Defendants, and each of them, meaningfully educating their customers and all individuals impacted by the Data Breach about the threats they face with regard to the security of their Private Information, as well as the steps Defendants' customers should take to protect Plaintiffs' and Class Members' Private Information going forward.

202. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at PROGRESS and/or PBI. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

203. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial,

continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

204. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at PROGRESS and/or PBI, thus preventing future injury to Plaintiffs and Class Members whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

1. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

2. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

3. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

4. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

5. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

6. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

7. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: July 3, 2023

Respectfully submitted,

/s/ Ramin R. Younessi

LAW OFFICE OF RAMIN R YOUNESSI
A PROFESSIONAL LAW CORP.
Ramin R. Younessi, Esq.
Heather N. Phillips, Esq.
3435 Wilshire Boulevard, Suite 2200
Los Angeles, CA 90010
Tel: (213) 480-6200
E: ryounessi@younessilaw.com
hphillips@younessilaw.com